ISSN: 2692-5397
Modern Concepts in Material Science
DOI: 10.33552/MCMS.2024.05.000618
Iris Publishers

Research Article

Guardians of App Integrity: A Machine Learning Approach to Detecting Spam Reviews on the Google Play Store

Hina Ayub[1], Murad Ali Khan[2]*

[1]*Interdisciplinary Graduate Program in Advanced Convergence Technology and Science, Jeju National University, Jeju 63243, Republic of Korea*

[2]*Department of Computer Engineering, Jeju National University, Jeju 63243, Republic of Korea*

***Corresponding author:** Murad Ali Khan, Department of Computer Engineering, Jeju National University, Jeju 63243, Republic of Korea*

Received Date: **January 11, 2024**

Published Date: **January 19, 2024**

Abstract

Nowadays, most Android users check reviews on the Google Play Store [1] before downloading applications. Normally, when a user is required to download an application from Google Play, he/she checks reviews of the required application before downloading the application. If the maximum opinions of the previous users are good, then the user downloads the application. If maximum opinions are against the application, the user ignores the application and checks other applications. Positive opinions can result in financial benefits and fame for developers. Most local developers make small teams to give fake reviews to their Apps to gain a good ranking in Google Play. When local users visit Google Play to download the required Apps, they look for top-ranked applications on Google Play. Most of the time, due to fake reviews, local applications get top ranking in Google Play, and due to good ranking, local users download it, which does not fulfill their requirements. So, we are investigating a system to detect spam reviews on the Google Play Store application using ML techniques. In this study, we are using dataset user complaints of wearable apps dataset [2]. After this, we are developing a desktop application where users can see which reviews are spam and which are real. Our system is also helpful for researchers who are dealing with review studies. Users can enter his/her reviews with some constraints, and our system gives them output that will show which reviews are real and which are fake.

Keywords: Google Play Store, Android applications, User reviews, Spam detection, Machine learning techniques, Wearable apps dataset.

Introduction

In the contemporary digital landscape, the Google Play Store is a paramount platform for Android users seeking applications catering to their diverse needs. The reviews provided by other users often influence users' decision-making process in selecting an application. In this era of information abundance, users rely on these reviews to gauge the credibility and functionality of an application before committing to a download. However, the integrity of this review system has been compromised by the proliferation of spam reviews, creating a challenging landscape for both users and developers.

When users are confronted with selecting an application from the vast array available on the Google Play Store, the abundance of positive reviews typically sways their decision to favour an application. Conversely, a preponderance of negative opinions can dissuade potential users from downloading an application. This symbiotic relationship between reviews and user decisions underscores the critical role that appraisals play in the success or failure of applications in the highly competitive digital marketplace. In pursuing appraisals that confer financial benefits and acclaim to developers, a disconcerting trend has emerged - manipulating reviews artificially. In order to elevate their applications to the upper echelons of Google Play Store rankings, local developers often assemble small teams to fabricate positive reviews. This deceptive practice not only misguides potential users but also compromises the integrity of the review system.

We comprehensively investigate spam review detection on the Google Play Store to address this challenge. Our study employs machine learning techniques and leverages the Wearable Apps dataset, derived from user complaints, as a foundational resource for training and validation. With its increasing prevalence and reliance on accompanying applications, Wearable technology serves as a pertinent domain for our investigation. The crux of our research lies in developing a robust desktop application designed to empower users to distinguish between authentic and spam reviews. By implementing a machine learning model trained on a diverse dataset of user complaints specific to wearable apps, our system aims to provide users with nuanced insights into the legitimacy of reviews. This initiative not only safeguards users from the pitfalls of misleading reviews but also offers a valuable tool for researchers delving into the intricate dynamics of user appraisals.

In the subsequent sections of this paper, we delve into the methodology employed for training and validating our machine learning model, the intricacies of the Wearable Apps dataset, and the design and functionality of our desktop application. Through this multifaceted approach, we aspire to contribute a robust solution to the pervasive issue of spam reviews on the Google Play Store, fostering a more transparent and trustworthy digital ecosystem for users and developers alike.

Literature Review

The persistent issue of spam detection has long been a focal point of research across various domains, including spam reviews [3-5], e-mail spam [6-9], social spam [10-13], and spam bots [14-15]. An exhaustive review of recent literature was undertaken to gain a comprehensive understanding of the domain problem, utilizing databases such as Google Scholar, Web of Science, Research Gate, Science Direct, Semantic Scholar, IEEE Xplore, Springer, ACM, and others. The detection of spam reviews is commonly treated as a binary classification problem, addressed through diverse methods such as machine learning and deep learning. This discussion delves into various research articles that employ distinct approaches for detecting spam messages.

A noteworthy study [16] offers an in-depth analysis of recent spam detection methods, encompassing aspects such as datasets, features, machine learning and deep learning models, performance measures, and merits and demerits. Additionally, another research article [17] provides a comprehensive review of practical deep learning techniques, specifically recurrent neural networks, and convolutional neural networks, focusing on the SMS corpus to develop a binary spam classifier. Further contributing to the literature, [18] explores spam email detection with a classification approach using machine learning techniques for abnormal detection. The study offers a thorough review and analysis of various machine learning models and features employed in diverse approaches for abnormal email detection, presenting valuable insights into future research directions and potential obstacles in this evolving field.

In another study presented by [19], the authors developed a cognitive spam detection model that detects and removes spam pages during web link rank calculation. The proposed model spots web spam with the help of a Short-term network based on link features. This training result achieved an accuracy of 95.25%, as more than 111000 hosts were correctly classified. Similar research in the same domain was conducted by [20], where the author used different techniques to extract highly connected features from email content and determine which features are more helpful in detecting abnormal traffic. The author used various state-of-the-art machine learning algorithms to check the performance of the selected features and achieved 99% accuracy in the detection of spam emails.

This study [21] investigated and analyzed online reviews for spam detection based on different machine learning algorithms and proposed a model using a stochastic-gradient-descent algorithm to predict abnormal reviews. The model uses bagging and boosting techniques to overcome variance and bias problems. Moreover, for the selection of optimal features from a huge feature space, some rules-based regular expressions are generated. Finally, experiments on the hotel reviews dataset proved the effectiveness of the study. Xianyu, one of the largest second-hand product seller apps in China, faces spam reviews by spammers to misguide customers. A large-scale anti-spam model based on convolutional graph networks is developing to predict spam advertisements on the Xianyu app [22]. The model is deployed to process Millions of data on a daily basis. The real-time experiments of the model showed that the proposed model can effectively detect spam reviews. Another study proposed by [23] is based on only text data and a self-extracted feature set. A benchmark data set for model evaluation consists of 4,827 Not-Spam SMS and 747 Spam SMS, a remarkable performance of 99.44% accuracy was achieved. Bio-inspired techniques like genetic algorithms and particle swarm optimization were developed by [24] to detect spam emails. Multinomial Naïve Bayes integrated with Genetic Algorithm gives the best performance.

Proposed Methodology

Our research aims to develop a robust system capable of detecting spam reviews on the Google Play Store using machine learning techniques. To achieve this, we propose a comprehensive methodology involving data preprocessing, feature extraction, model training, and results for review analysis.

The Architecture of the Methodology

Our proposed methodology encompasses a well-defined architectural framework aimed at systematically addressing the challenges of spam reviews on the Google Play Store. The architecture unfolds in a series of intricately connected steps, each contributing to the overall robustness of our approach, as shown in Figure 1.

Data Acquisition: The process begins with acquiring raw review data, a crucial step to ensure the authenticity and relevance of the dataset. This raw data represents diverse user complaints regarding wearable apps, forming the foundation for subsequent analysis.

Data Preprocessing: The acquired raw data undergoes a meticulous data preprocessing phase comprising several crucial steps:

a. Data Cleaning: In this step, we eliminate noise and inconsistencies in the dataset, ensuring a high-quality foundation for subsequent analysis.

b. Data Attributes Selection: Relevant attributes are carefully selected to focus the analysis on key aspects, enhancing the efficiency of our model.

c. Data Attribute Transformation: Transformation techniques are applied to mold data attributes into suitable formats for analysis, promoting uniformity and compatibility.

d. Feature Engineering: The extraction of meaningful features from the data occurs in this step, encompassing textual elements and metadata to capture the nuanced aspects of each review.

Data Resampling: Recognizing the challenge of imbalanced data, our methodology employs advanced resampling techniques to address this issue. Resampling methods, including Random Over-Sampling (ROS), Adaptive Synthetic Sampling (ADASYN), SMOTE (Synthetic Minority Over-sampling Technique), Tomek links, and SMOTE combined with Tomek links, are systematically applied to ensure a balanced representation of authentic and spam reviews.

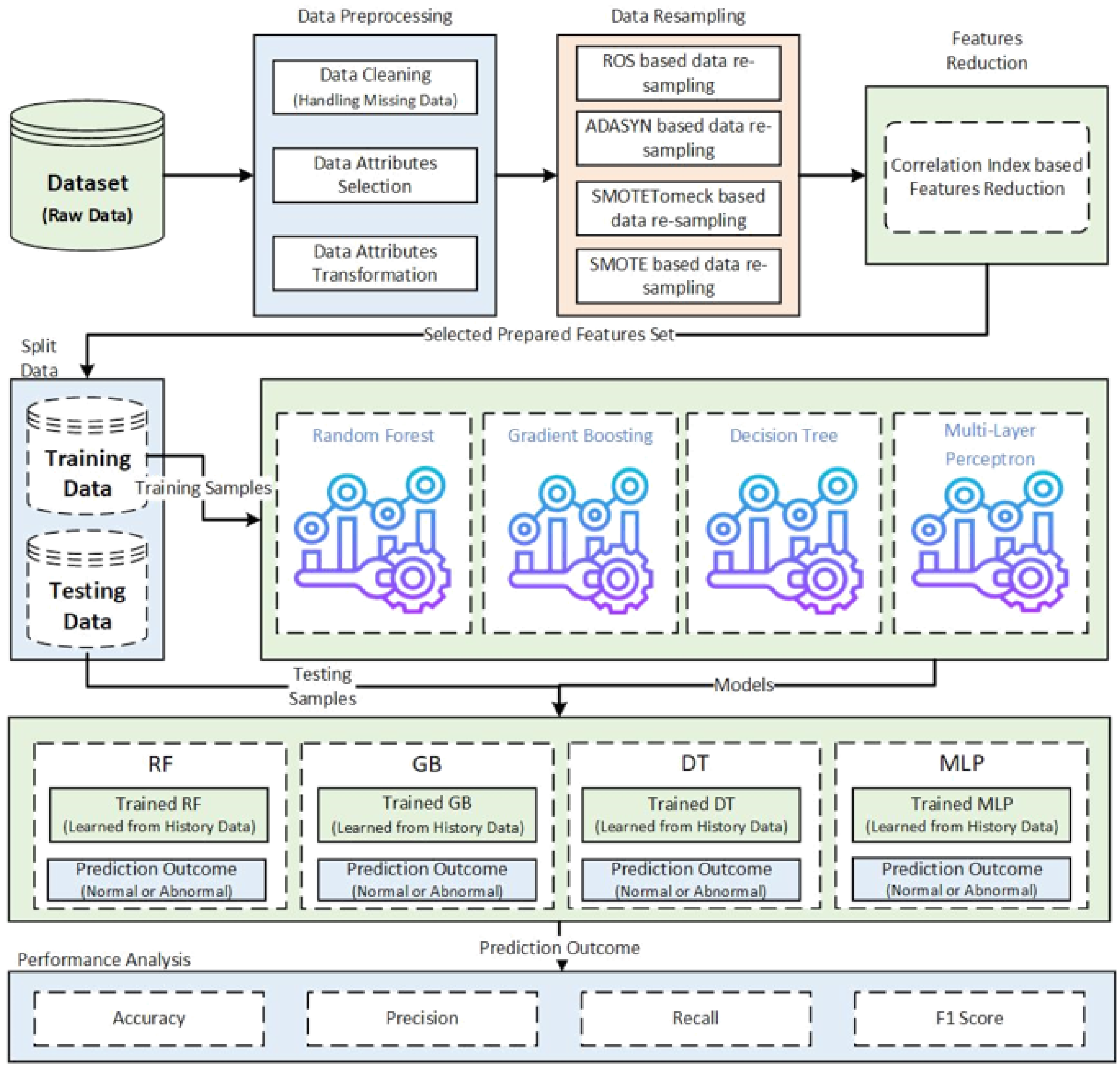
Data Preprocessing
Data Resampling
Features Reduction
Dataset
(Raw Data)
Data Cleaning
(Handling Missing Data)
Data Attributes Selection
Data Attributes Transformation
ROS based data re-sampling
ADASYN based data re-sampling
SMOTETomeck based data re-sampling
SMOTE based data re-sampling
Correlation Index based Features Reduction
Selected Prepared Features Set
Split Data
Training Data
Training Samples
Testing Data
Random Forest
Gradient Boosting
Decision Tree
Multi-Layer Perceptron
Testing Samples
Models
RF
GB
DT
MLP
Trained RF (Learned from History Data)
Trained GB (Learned from History Data)
Trained DT (Learned from History Data)
Trained MLP (Learned from History Data)
Prediction Outcome (Normal or Abnormal)
Prediction Outcome
Performance Analysis
Accuracy
Precision
Recall
F1 Score

Figure 1: A complete flow of the proposed spam detection mechanism.

Feature Reduction: A feature reduction step is implemented to streamline the dataset and enhance the efficiency of our model. Correlation analysis is conducted to identify and retain the most informative features while discarding redundant or highly correlated ones.

Machine Learning Model Training: The prepared data is then split into training and testing sets. This partitioning allows us to train our machine-learning models on the training data. Various algorithms, including Random Forest, Gradient Boosting, Decision Tree, and Multi-Layer Perceptron, are explored to identify the most effective model for discriminating between genuine and spam reviews.

Model Evaluation: Post-training, the models are rigorously evaluated using the test data to ascertain their performance metrics. These metrics, including accuracy, precision, recall, and F1 score, comprehensively understand each model's efficacy in distinguishing between authentic and spam reviews.

Results Reporting: The final step involves reporting the outcomes of our methodology. Detailed results obtained through the evaluation of trained models are presented to provide insights into the effectiveness of our approach. This reporting stage serves as a crucial feedback loop, informing potential adjustments and improvements to the overall methodology.

The architectural flow of our methodology ensures a systematic and thorough approach to detecting spam reviews on the Google Play Store. By integrating data preprocessing, resampling, feature reduction, machine learning model training, and evaluation, our methodology forms a comprehensive solution to address the nuanced challenges posed by the prevalence of spam reviews in the digital ecosystem.

Results And Comparative Analysis

This section delves into the performance evaluation of our proposed spam review detection methodology on the Google Play Store. Through a thorough examination of key performance metrics like accuracy, precision, recall, and F1 score, we present a comprehensive comparative analysis of four machine learning models, shedding light on their respective strengths and contributions to the effectiveness of our approach.

Performance Measures:

We employ a set of key performance measures to evaluate the effectiveness of our proposed methodology for spam review detection on the Google Play Store. These measures offer a comprehensive understanding of the model's performance beyond a single metric. The following metrics are considered.:

Accuracy: Accuracy measures the overall correctness of the model by considering both true positives and true negatives.

$$\text{Accuracy} = \frac{\text{True Positives} + \text{TrueNegatives}}{\text{TotalPredications}}$$

Precision: Precision reflects the accuracy of positive predictions, indicating how many of the predicted positives are actually true positives.

$$\text{Precision} = \frac{\text{TruePositives}}{\text{TruePositives} + \text{FalsePositives}}$$

Recall: Recall focuses on the model's ability to capture all actual positives, expressing the ratio of correctly predicted positives to all actual positives.

$$\text{Recall} = \frac{\text{TruePositives}}{\text{TruePositives} + \text{FalseNegatives}}$$

F1 Score: F1 score balances precision and recall, providing a harmonic mean that is especially useful when there is an imbalance between false positives and false negatives.

$$\text{F1 Score} = 2 * \frac{\text{Precision} * \text{Recall}}{\text{Precision} + \text{Recall}}$$

C. Comparative Analysis:

Table 1: A comparative analysis table for ML models.

Model	Accuracy (%)	Precision (%)	Recall (%)	F1 Score (%)
Random Forest	99.4	87.4	93.3	90.2
Gradient Boosting	99.3	86	89.9	87.9
Decision Tree	91.5	79.2	96.9	87.2
Multi-Layer Perceptron	**99.7**	**99.4**	**99.9**	**99.7**

Our methodology's performance is assessed by applying four machine learning models: Random Forest, Gradient Boosting, Decision Tree, and Multi-Layer Perceptron. The results are compiled and presented in the following comparative analysis Table 1.

The machine learning model results for spam review detection on the Google Play Store present a compelling picture of their individual strengths. With an accuracy of 99.4%, Random Forest excels in achieving an optimal balance between precision (87.4%) and recall (93.3%). This suggests that the model is highly accurate in correctly classifying authentic and spam reviews, emphasizing minimizing false negatives. Gradient Boosting, with an accuracy of 99.3%, showcases a robust performance with commendable recall

Citation: Hina Ayub, Murad Ali Khan*. Guardians of App Integrity: A Machine Learning Approach to Detecting Spam Reviews on the Google Play Store. Mod Concept Material Sci. 5(4): 2024. MCMS. MS.ID.000618. DOI: 10.33552/MCMS.2024.05.000618

(89.9%) and a well-balanced F1 score of 87.9%. While it slightly lags behind Random Forest in precision, Gradient Boosting remains a formidable contender with a comprehensive ability to capture actual spam reviews.

On the other hand, the Decision Tree, with an accuracy of 91.5%, exhibits a unique strength in recall (96.9%), surpassing other models in capturing a substantial proportion of true positives. This makes the Decision Tree particularly effective in minimizing false negatives. Lastly, the Multi-Layer Perceptron outshines others with exceptional accuracy (99.7%), precision (99.4%), and recall (99.9%). Its high F1 score of 99.7% underscores a near-perfect balance between precision and recall, making it an outstanding choice for applications prioritizing overall performance. In summary, the results provide valuable insights into the nuanced strengths of each model, aiding in the selection of an optimal model based on specific priorities and application requirements. A visual representation of the overall results is illustrated in Figure 2.

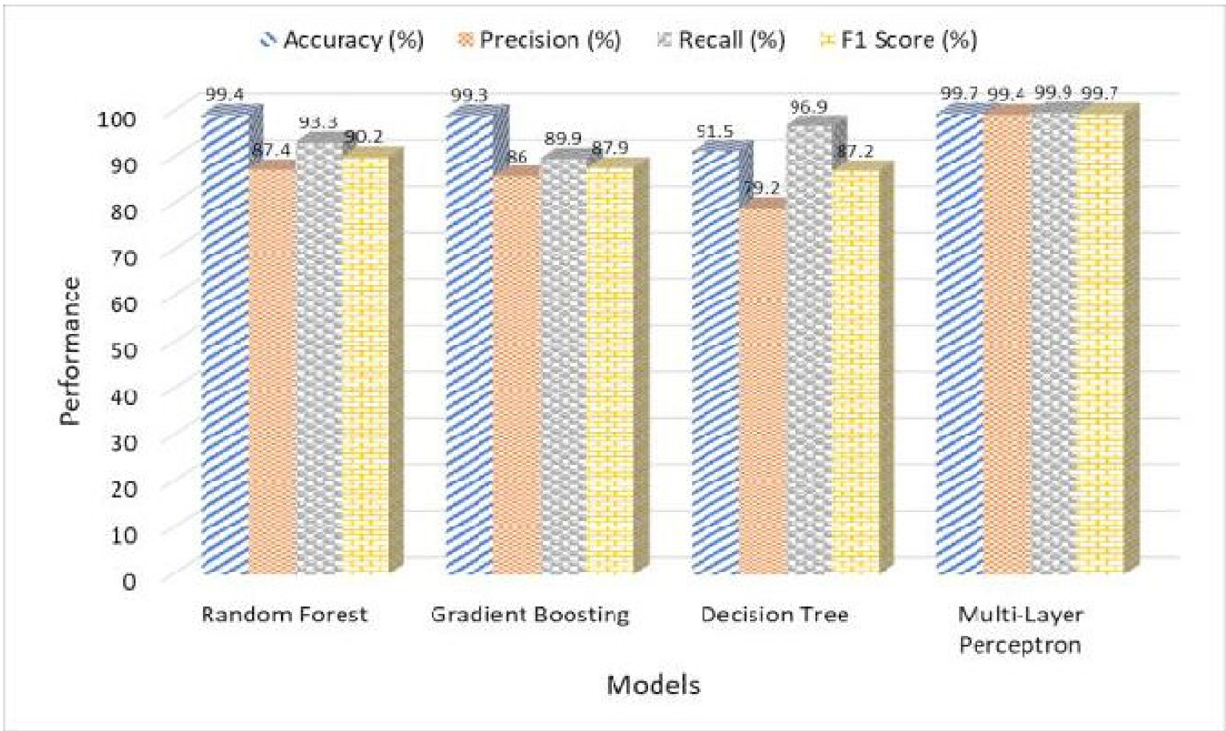

Figure 2: A visual representation of the ML model results.

Conclusion

In conclusion, the results of our spam review detection methodology on the Google Play Store underscore the effectiveness of machine learning models in mitigating the impact of deceptive reviews. Random Forest and Multi-Layer Perceptron emerge as robust performers, showcasing high accuracy and a harmonious balance between precision and recall. The findings provide valuable insights for developers seeking reliable tools for app evaluation and users navigating the vast app landscape. The contribution of this research lies in offering a systematic approach to address the challenges posed by spam reviews, fostering a more credible digital marketplace. Future work involves refining the methodology with additional algorithms, advancing feature engineering, and exploring real-time data integration. Collaborative efforts with stakeholders could propel the implementation of our approach, contributing to a more transparent and resilient digital ecosystem in the realm of mobile app reviews.

Acknowledgment

None.

Conflicts of Interest

None.

References

1. Eler, Marcelo Medeiros, Leandro Orlandin, Alberto Dumont Alves Oliveira (2019) Do Android app users care about accessibility? an analysis of user reviews on the Google play store. Proceedings of the 18th Brazilian symposium on human factors in computing systems.
2. Venkatakrishnan, Swathi, Abhishek Kaushik, Jitendra Kumar Verma (2020) Sentiment analysis on google play store data using deep learning. Applications of Machine Learning pp. 15-30.
3. Crawford, Michael, Joseph D Prusa, Aaron N Richter, Hamzah Al Najada, et al. (2015) Survey of review spam detection using machine learning techniques. Journal of Big Data 2(1): 1-24.
4. Heydari Atefeh, Mohammad ali Tavakoli, Naomie Salim, Zahra Heydari (2015) Detection of review spam: A survey. Expert Systems with Applications 42(7): 3634-3642.

5. Hussain Naveed, Hamid Turab Mirza, Ghulam Rasool, Ibrar Hussain, Mohammad Kaleem, et al. (2019) Spam review detection techniques: A systematic literature review. Applied Sciences 9(5): 987.

6. Bhowmick Alexy, Shyamanta M Hazarika (2018) E-mail spam filtering: a review of techniques and trends. Advances in Electronics, Communication and Computing: ETAEERE-2016: 583-590.

7. Dada Emmanuel Gbenga, Joseph Stephen Bassi, Haruna Chiroma, Shafii Muhammad Abdulhamid, Adebayo Olusola Adetunmbi, et al. (2019) Machine learning for email spam filtering: review, approaches and open research problems. Heliyon 5(6): e01802.

8. Gangavarapu Tushaar, C D Jaidhar, Bhabesh Chanduka (2020) Applicability of machine learning in spam and phishing email filtering: review and approaches. Artificial Intelligence Review 53: 5019-5081.

9. Karim Asif, Sami Azam, Bharanidharan Shanmugam, Krishnan Kannoorpatti, And Mamoun Alazab, et al. (2019) A comprehensive survey for intelligent spam email detection. IEEE Access 7: 168261-168295.

10. Adewole Kayode Sakariyah, Nor Badrul Anuar, Amirrudin Kamsin, Kasturi Dewi Varathan, Syed Abdul Razak, et al. (2017) Malicious accounts: Dark of the social networks. Journal of Network and Computer Applications 79: 41-67.

11. Imam Niddal H, Vassilios G Vassilakis (2019) A survey of attacks against twitter spam detectors in an adversarial environment. Robotics 8(3): 50.

12. Kaur Ravneet, Sarbjeet Singh, Harish Kumar (2018) Rise of spam and compromised accounts in online social networks: A state-of-the-art review of different combating approaches. Journal of Network and Computer Applications 112: 53-88.

13. Wu Tingmin, Sheng Wen, Yang Xiang, Wanlei Zhou (2018) Twitter spam detection: Survey of new approaches and comparative study. Computers & Security 76: 265-284.

14. Gallwitz Florian, Michael Kreil (2021) The Rise and Fall of'Social Bot'Research. Available at SSRN 3814191.

15. Latah Majd (2020) Detection of malicious social bots: A survey and a refined taxonomy. Expert Systems with Applications 151: 113383.

16. Rao Sanjeev, Anil Kumar Verma, Tarunpreet Bhatia (2021) A review on social spam detection: challenges, open issues, and future directions. Expert Systems with Applications 186: 115742.

17. Annareddy Sunil, Srikanth Tammina (2019) A comparative study of deep learning methods for spam detection. 2019 third international conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC). IEEE.

18. Mansoor R A Z A, Nathali Dilshani Jayasinghe, Muhana Magboul Ali Muslam (2021) A comprehensive review on email spam classification using machine learning algorithms. 2021 International Conference on Information Networking (ICOIN). IEEE.

19. Makkar Aaisha, Neeraj Kumar (2020) An efficient deep learning-based scheme for web spam detection in IoT environment. Future Generation Computer Systems 108: 467-487.

20. Gangavarapu Tushaar, C D Jaidhar, Bhabesh Chanduka (2020) Applicability of machine learning in spam and phishing email filtering: review and approaches. Artificial Intelligence Review 53: 5019-5081.

21. Sultana Naznin, Sellappan Palaniappan (2020) Deceptive Opinion Detection Using Machine Learning Techniques. International Journal of Information Engineering &Electronic Business 12(1): 1-7.

22. Li Ao, Zhou Qin, Runshi Liu, Yiqun Yang, Dong Li, et al. (2019) Spam review detection with graph convolutional networks. Proceedings of the 28th ACM International Conference on Information and Knowledge Management.

23. Roy Pradeep Kumar, Jyoti Prakash Singh, Snehasish Banerjee (2020) Deep learning to filter SMS Spam. Future Generation Computer Systems 102: 524-533.

24. Gibson Simran, Biju Issac, Li Zhang, Seibu Mary Jacob (2020) Detecting spam email with machine learning optimized with bio-inspired metaheuristic algorithms. Ieee Access 8: 187914-187932.